MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON

GENERAL CONTROLS OF THE OFFENDER MANAGEMENT NETWORK INFORMATION SYSTEM

DEPARTMENT OF CORRECTIONS AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

December 2014

Doug A. Ringler, C.P.A., C.I.A.
AUDITOR GENERAL

471-0592-07F

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

– Article IV, Section 53 of the Michigan Constitution

Audit report information can be accessed at:
http://audgen.michigan.gov

OAG

Office of the Auditor General

201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • http://audgen.michigan.gov

Doug A. Ringler, C.P.A., C.I.A.
Auditor General

December 11, 2014

Mr. Daniel H. Heyns, Director
Department of Corrections
Grandview Plaza Building
Lansing, Michigan
and
Mr. David B. Behen
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. Heyns and Mr. Behen:

This is our report on our follow-up of the 2 material conditions (Findings 1 and 4) and 2 corresponding recommendations reported in the performance audit of General Controls of the Offender Management Network Information System, Department of Corrections (DOC) and Department of Information Technology (DIT). That audit report was issued and distributed in December 2007. Additional copies are available on request or at <http://audgen.michigan.gov>.

In March 2010, subsequent to our performance audit, Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management, and Budget (DTMB). It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and unexpended balances of appropriations, allocations, or other funds of DIT to DTMB and abolished DIT.

This report contains an introduction; our purpose of follow-up; a background; our scope; follow-up conclusions, results, recommendation, and agency response; and a glossary of abbreviations and terms.

Our follow-up disclosed that DOC and DTMB had complied with 1 recommendation and had partially complied with 1 recommendation. A reportable condition exists related to Offender Management Network Information System access (Finding 1). As a result, we have issued a rewritten recommendation.

We appreciate the courtesy and cooperation extended to us during our follow-up. If you have any questions, please call me or Laura J. Hirst, C.P.A., Deputy Auditor General.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

FOLLOW-UP REPORT
GENERAL CONTROLS OF THE
OFFENDER MANAGEMENT NETWORK INFORMATION SYSTEM
DEPARTMENT OF CORRECTIONS AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

FOLLOW-UP REPORT
GENERAL CONTROLS* OF THE OFFENDER MANAGEMENT NETWORK INFORMATION SYSTEM
DEPARTMENT OF CORRECTIONS
AND DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

INTRODUCTION

This report contains the results of our follow-up of the material conditions* and corresponding recommendations reported in our performance audit* of General Controls of the Offender Management Network Information System, Department of Corrections (DOC) and Department of Information Technology (DIT), (471-0592-07), which was issued and distributed in December 2007. That audit report included 2 material conditions (Findings 1 and 4) and 3 reportable conditions*. This report also contains DOC's plan to comply with our prior audit recommendations for the 2 material conditions, which was required by the *Michigan Compiled Laws* and administrative procedures to be developed within 60 days after release of the December 2007 audit report.

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether DOC and the Department of Technology, Management, and Budget (DTMB) had taken appropriate corrective measures in response to the 2 material conditions and corresponding recommendations noted within our December 2007 audit report.

** See glossary at end of report for definition.*

BACKGROUND

Offender Management Network Information System (OMNI)

OMNI is an information processing system that DOC uses to store and manage offender* and employee data. As of December 2013, OMNI contained data for 43,704 prisoners, 10,540 parolees, and an average of 47,526 probationers. OMNI also contains data for some offenders who have not yet been sentenced.

DOC uses OMNI to process the intake of prisoners into the correctional system and to manage the supervision of parolees and probationers. During the intake of prisoners, DOC enters prisoner and sentencing information into OMNI. The sentencing information is transferred electronically to DOC's Corrections Management Information System (CMIS). CMIS performs the computation of prisoner release dates. For parolees and probationers, DOC uses OMNI to track and record the parole violation process, Parole Board* consideration process, and community supervision. OMNI also contains DOC employee information.

OMNI data is used by DOC's Offender Tracking Information System (OTIS) and the Michigan Department of State Police's Law Enforcement Information Network (LEIN). OTIS provides information to the public about offenders currently or previously in a Michigan prison or on parole or probation under the supervision of DOC. LEIN provides offender information to criminal justice agencies.

OMNI has approximately 13,000 users, including DOC employees, Michigan Department of State Police and other State of Michigan employees, and contractors. There are 97 user profiles that DOC assigns to users that determine what OMNI modules and data a user can access. Some of the OMNI modules include offender intake, reception center in-processing, offender tracking, offender callout*, probation case administration, and Parole Board administration.

Department of Technology, Management, and Budget (DTMB)

Executive Order No. 2009-55, effective March 21, 2010, abolished DIT and renamed the Department of Management and Budget as DTMB. DTMB provides information technology* support services to DOC for OMNI. The services include system development and maintenance, database and operating system security and administration, and backup and recovery management.

** See glossary at end of report for definition.*

SCOPE

Our fieldwork was performed primarily during May through August 2014. We interviewed employees from DOC and DTMB to determine the status of compliance with our audit recommendations. Also, we reviewed the list of individuals authorized to grant user access, along with user access lists. In addition, we reviewed policies and procedures related to change requests and granting user access.

FOLLOW-UP CONCLUSIONS, RESULTS, RECOMMENDATION, AND AGENCY RESPONSE

EFFECTIVENESS OF ACCESS CONTROLS*

SUMMARY OF THE DECEMBER 2007 FINDING

1. OMNI Access

DOC had not established a comprehensive information systems security program and effective access controls over OMNI. As a result, DOC cannot ensure the security and integrity* of OMNI data. Our review of OMNI access controls disclosed the following weaknesses:

a. DOC had not established an information security officer position.

b. DOC did not restrict DIT application development staff from administrative access to OMNI.

c. DOC did not have documented policies and procedures for assigning and authorizing access to data. We noted:

(1) DOC did not have a process to ensure that correctional facility staff requesting and approving access had the authority to do so.

(2) DOC did not provide written policies to correctional facility staff to provide guidance on assigning the appropriate access for a user's job function.

d. DOC did not have an effective process to remove user access. We noted:

(1) DOC did not remove inactive user accounts.

(2) DOC did not remove access for all terminated State employees.

** See glossary at end of report for definition.*

e. DOC did not ensure appropriate assignment of OMNI user profiles* and accounts. We noted:

   (1) DOC did not document the user profiles that are appropriate for each job responsibility.

   (2) DOC did not maintain documentation that user access had been reviewed and approved for a valid business need.

   (3) DOC did not identify users who were inappropriately assigned multiple user accounts.

f. DOC did not have secure OMNI administrator accounts.

g. DOC did not retain logs of security background checks and security agreements for contractors and other non-DOC State employees at DOC's Automated Data Systems Section (ADSS) where access was granted.

RECOMMENDATION (AS REPORTED IN DECEMBER 2007)

We again recommend that DOC establish a comprehensive information systems security program and effective access controls over OMNI.

AGENCY PLAN TO COMPLY*

DOC agrees and will comply. DOC informed us that the information security officer position had recently been approved and this position would establish security policies, standards, and operating procedures to safeguard OMNI data. Also, DOC will develop an appropriate profile for DIT application development staff. In addition, DOC will require correctional facilities to identify authorized requestors who have the authority to request new user access or modifications to a user's access. Further, DOC will implement policies and procedures to suspend access for inactive OMNI user accounts and remove access for terminated employees. Also, DOC will take steps to improve assignment of appropriate OMNI user profiles based upon an employee's job responsibilities and audit all non-DOC OMNI users to confirm that documentation is available within ADSS to validate user access for business needs. In addition, DOC has reduced the number of security

** See glossary at end of report for definition.*

administrators and will work to further limit the number of ADSS security administrators with the development of a security unit. Further, DOC began retaining logs of security background checks and security agreements for non-DOC OMNI users.

FOLLOW-UP CONCLUSION

We concluded that DOC partially complied with the recommendation and a reportable condition exists.

FOLLOW-UP RESULTS

Our follow-up disclosed:

a. Regarding part a. of the finding, DOC complied with the recommendation. DOC appointed a security officer in 2009 with the responsibility and authority to implement information security policies, standards, and operating procedures for safeguarding all DOC information resources.

b. Regarding part b. of the finding, DOC complied with the recommendation. We noted that DOC, in conjunction with DTMB, had transferred security administration of OMNI from DTMB to DOC in 2009. We reviewed privileged access* to OMNI and determined that only appropriate staff had access rights to view and modify OMNI data.

c. Regarding part c. of the finding, DOC partially complied with the recommendation. We noted:

    (1) DOC did not ensure that correctional facility staff requesting and approving access to OMNI had the authority to do so. We identified 1 (10%) of 10 judgmentally selected authorized requestors who was no longer employed by the facility for which he was authorized to approve access.

    (2) DOC implemented a policy for the assignment of access appropriate for a user's job function. We reviewed the policy and determined that it provided sufficient guidance on who is authorized to request access and the appropriate level of access for a user's job function.

** See glossary at end of report for definition.*

d. Regarding part d. of the finding, DOC partially complied with the recommendation. We noted:

(1) DOC did not remove inactive user accounts. As of August 6, 2014, we identified 6,126 user accounts that had not accessed OMNI in the past 90 days. DOC informed us that it had not removed the inactive user accounts because the users may need to access OMNI again. However, we noted 99 users who had not accessed OMNI since 2009. We noted that none of the inactive users had high-risk user accounts with access to critical data.

(2) DOC did not remove access for all terminated State employees. As of July 19, 2014, we identified 119 user accounts that were assigned to former State employees. DOC informed us that it had not removed the access of the terminated employees because it reviews human resources reports quarterly and had not reviewed the most recent report as of the time of our follow-up. However, we noted users who had terminated employment in 2011, 2012, and 2013 whose access had not been removed. Of the 119 user accounts, we identified no high-risk user accounts with access to critical data.

e. Regarding part e. of the finding, DOC partially complied with the recommendation. We noted:

(1) DOC documented user profiles and defined which profiles were appropriate for each job responsibility. We obtained a list of OMNI user profiles and verified that DOC had defined and documented the purpose of each profile.

(2) DOC did not have documentation of the business need for all external OMNI users. We randomly selected 15 external OMNI users and determined that DOC did not have documentation of the business need to access OMNI for 2 (13%) non-DOC employees.

(3) DOC implemented a process to ensure that OMNI users were not inappropriately assigned multiple accounts. We reviewed the list of OMNI

profiles and users at each facility and did not identify any users who were inappropriately assigned multiple accounts.

f. Regarding part f. of the finding, DOC partially complied with the recommendation. DOC reduced the number of OMNI administrator accounts from 22 to 7. However, it did not maintain documentation that it periodically monitored the account activity to ensure accountability for administrator actions. DOC informed us that it periodically reviews the accounts, but it had not established a time frame for how often it conducts the review nor is the review documented.

g. Regarding part g. of the finding, DOC complied with the recommendation. DOC retained logs of security background checks and security agreements for contractors and other non-DOC State employees with access to OMNI. We randomly selected 15 external OMNI users and verified that DOC retained the security background checks and security agreements for all of our randomly selected users.

FOLLOW-UP RECOMMENDATION

We recommend that DOC continue to establish effective access controls over OMNI by ensuring that only appropriate individuals have access to OMNI, restricting the ability to request and approve access to OMNI, and maintaining documentation of its review of administrator accounts.

FOLLOW-UP AGENCY RESPONSE

DOC provided us with the following response:

DOC agrees with the recommendation.

Regarding part c., DOC agrees that there was one person on the authorized requester list who was retired from State service for a few months. DOC had a process in place whereby Human Resources and facilities/offices notify the user code maintenance unit when staff terminate employment with DOC. The one person was on the most recent Human Resources quarterly report and the user code maintenance unit was aware of the person's retirement. However, the person was inadvertently left on the list.

Regarding part d., DOC agrees that it did not remove accounts that OMNI users had not accessed in the past 90 days. However, DOC safeguards these accounts using password resets rather than by removing the accounts because employees working within DOC's 24/7 operation may be thrust into a job duty that mandates the use of OMNI at any given time to complete certain assignments related to the safety and security of the facility. To improve the control, the DOC Security Officer will work with facilities/offices to periodically review inactive accounts to confirm users' continued employment and need for the account.

Regarding part e., DOC agrees and will continue to document the business need for external OMNI users. DOC's Security Officer will periodically review external user files to ensure that a business case is documented.

Regarding part f., DOC agrees. The Security Officer will maintain documentation for periodic reviews of administrator account activity.

EFFECTIVENESS OF CHANGE CONTROLS*

SUMMARY OF THE DECEMBER 2007 FINDING

4. Change Control Process

DIT and DOC had not developed a comprehensive change control process for OMNI. As a result, DIT and DOC could not ensure that OMNI program files, database software, and operating system software were protected from corruption and unauthorized changes. Our review disclosed:

a. DOC had not fully established effective controls over program and database changes.

b. DIT did not fully ensure a proper segregation of duties* for the change control process.

c. DIT did not maintain an effective audit trail of all program and database changes.

* *See glossary at end of report for definition.*

d. DIT did not have a documented process for making emergency program and database changes.

RECOMMENDATION (AS REPORTED IN DECEMBER 2007)

We recommend that DIT and DOC develop a comprehensive change control process for OMNI.

AGENCY PLAN TO COMPLY

DOC agrees and will comply. DOC will modify its change request forms to include the name of the person who requested the change, the name of the person within ADSS who is requesting the change to be implemented, and the name of the ADSS manager who approved the request. Upon staff providing test acceptance in the test application environment, an ADSS manager will document his/her authorization to implement and notify DIT that the change is authorized for implementation.

FOLLOW-UP CONCLUSION

We concluded that DTMB and DOC had complied with the recommendation.

FOLLOW-UP RESULTS

Our follow-up disclosed:

a. Regarding part a. of the finding, DTMB and DOC updated the change request guidelines and implemented change order request (COR) procedure MDOC/AG* 001 in February 2009. We reviewed 20 COR forms and noted that all 20 contained the necessary management approvals for the program changes. In addition, all 20 CORs contained management approval of test results prior to the programs being moved to production.

b. Regarding part b. of the finding, DTMB implemented COR procedure MDOC/AG 001 in February 2009, which requires that the name of the individual who implemented a program or data change be documented on the COR form. We reviewed 20 COR forms and determined that DTMB used a proper segregation of duties for the initiating, authorizing, testing, and implementing of the changes.

** See glossary at end of report for definition.*

c. Regarding part c. of the finding, DTMB implemented COR procedure MDOC/AG 001 in February 2009, which requires that audit trails be documented on the COR form. We reviewed 20 COR forms and determined that DTMB maintained screen shots of changes made and test results on the COR forms.

d. Regarding part d. of the finding, DTMB implemented a policy in February 2013 that documented the conditions under which emergency changes are allowed to be made and the process for making those emergency program and database changes. We reviewed three emergency change requests and determined that the reason for each change request was appropriately documented, tested, and approved.

Glossary of Abbreviations and Terms

access controls

Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.

ADSS

Automated Data Systems Section.

agency plan to comply

The response required by Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100). The audited agency is required to develop a plan to comply with Office of the Auditor General audit recommendations and submit the plan within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

change controls

Controls that ensure that program, system, or infrastructure modifications are properly authorized, tested, documented, and monitored.

CMIS

Corrections Management Information System.

COR

change order request.

DIT

Department of Information Technology.

DOC

Department of Corrections.

DTMB

Department of Technology, Management, and Budget.

general controls

The structure, policies, and procedures that apply to an entity's overall computer operations. These controls include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.

information technology

Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.

integrity

Accuracy, completeness, and timeliness of data in an information system.

LEIN

Law Enforcement Information Network.

material condition

A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.

MDOC/AG

Michigan Department of Corrections/Attorney General.

offender

A prisoner, parolee, or probationer.

offender callout

A listing of offender activities for a given day.

OMNI

Offender Management Network Information System.

OMNI user profile

An OMNI application privilege assigned to a user that allows the user to view, enter, edit, or delete records in OMNI.

OTIS

Offender Tracking Information System.

Parole Board

The sole paroling authority for felony offenders committed to the jurisdiction of the Department of Corrections.

performance audit

An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability, and to facilitate decision making by parties responsible for overseeing or initiating corrective action.

privileged access

Extensive system access capabilities granted to persons responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.

reportable condition

A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.

segregation of duties

Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

STATE OF MICHIGAN · OFFICE of the AUDITOR GENERAL ·